INVESTMENT COMPANY INSTITUTE®
ICI Global
WASHINGTON, DC • BRUSSELS • LONDON • WWW.ICI.ORG

ICI VIEWPOINTS

FEBRUARY 17, 2016

Cybersecurity at Work: Creating Passwords That Are More Secure

By Peter Salmon

Welcome to the first in a monthly series of *ICI Viewpoints* focusing on sound practices in cybersecurity. Unless you have been hiding under a giant pebble in Australia's outback for the last 20 years, you certainly recognize the serious nature that this threat poses not only to the fund industry but to the entire nation. Seemingly not a day passes without a new data breach being revealed in the national news—but, just as frequently, many more occur that we do not learn about, for myriad reasons.

In this series of postings we will highlight some of the fundamental building blocks of establishing good "cybersecurity hygiene." We will not address more complex issues (say, the benefits of network segmentation or of ensuring maximum entropy in encryption), but will instead focus on the human element of cybersecurity and provide suggestions for sound practices, policies, and procedures. Though some might find these suggestions very elementary, remember that the vast majority of data breaches are initiated not by a sophisticated cybercriminal leveraging a heretofore unknown or unidentified vulnerability, but by bad actors who fool people into clicking on a link or opening an attachment—a very old and basic exploit.

Passwords That Pass Muster

Let's begin with a look at one of the most widely used—and misused—cybersecurity measures: the password.

The requirements for passwords can be weak, sometimes a sequence of characters not as long as the word itself. In addition, some users handle password security by writing them down and "hiding" them under keyboards, in desk drawers, or on random Post-it notes. While we can debate whether passwords should disappear altogether in favor of more secure and efficient systems of access to networks and websites, the fact remains that, for now, passwords are in our life and we need to be thoughtful about their use and storage. As such, allow me to suggest some prudent practices as well as some practices that should be considered.

Password creation. Passwords should be at least eight characters in length and include both upper- and lowercase letters, numbers, and special characters (&, #, %, and the like). These are known as complex passwords. Rather than a word, consider using a phrase (such as "the rain in Spain"), substituting numbers for vowels, and inserting a special character or two. In addition, if a site offers two-step verification, take full advantage of this extra security measure. Rather than just using a username and password to access the site, you will be sent, for example, a text message to your smartphone with a temporary number. You then use this number to access the site. This "out-of-band" step makes it much harder for a criminal to access a site using your credentials.

You also need to keep in mind what *not* to do. Avoid using birth dates, pet names, spouse names, ABCDEF, 12345, 11111, ABC123, password, passw0rd, baseball, football, passwords that use sequences in the standard QWERTY keyboard, etc. You may be rolling your eyes at this list, but many of them were identified as the most commonly used in 2015.

You also should avoid using the same password for multiple sites. If you follow this practice and one site is breached, the criminal who stole your credentials there will be unable to use that information to access a second site. This document from the SANS Institute provides good guidelines for creating passwords.

Password maintenance. Password "rotation," which requires users to change their password periodically, is typically suggested as a good security practice, but that advice can be too generic. What it really comes down to is the nature of the site and the value of the data that are stored there. For example, a password that provides access to a critical network, such as a corporate log-in, probably should be rotated periodically. But for sites that store less critical user data—say, a free-subscription magazine site—passwords

likely do not need to be rotated.

This basic guideline doesn't always apply, however, for two basic reasons. First, password rotation may not help in a situation where the password is protecting critical information but where a criminal is still able to breach the system by using someone else's credentials or by leveraging a network vulnerability. You won't know they've stolen your money or personal information until after the damage has been done. Second, studies have shown that users who rotate passwords frequently are more likely to create simple passwords that they can easily recall, rather than creating long, complex—and thus more secure—passwords. It's much better in both cases to create strong, complex passwords or phrases that only you can recall, and rotate only those passwords where the policy requires it.

If you are still worried that you won't recall your passwords, consider using a password manager that stores and encrypts your passwords. This way, you only need to remember the one strong password you create to access that password manager.

Our next post in this monthly series will ask, what is a four-letter word for an orderly arrangement of parts of an overall design or objective?

Other Posts in This Series:

- Cybersecurity at Work: Creating Passwords That Are More Secure
- Cybersecurity at Work: Incident Response Plans and What They Entail
- Cybersecurity at Work: Exercise Is Important
- Cybersecurity at Work: The Benefits of Information Sharing Networks
- Cybersecurity at Work: The Risks of Information Sharing
- Cybersecurity at Work: Keeping Secure When Away from the Office
- Cybersecurity at Work: I Know What You Know!
- Cybersecurity at Work: To Confront Evolving Threats, Flexibility Is Key

Peter Salmon is ICI's senior director of operations and technology.
